Listing of Claims

1. (Currently amended) A method of determining random values for ~~an~~ a stream cipher, comprising:

determining at least two sequential random values ~~for the stream cipher~~ in parallel utilizing a common S-box, the stream cipher comprising a logical combination of the random values and plaintext.

2. (Original) The method of Claim 1, wherein the step of determining at least two sequential random values in parallel utilizing a common S-box further comprises the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and accesses of the common S-box utilized to determine a second of the two sequential random values; and

modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

3. (Previously presented) The method of Claim 2, wherein the step of determining if a collision exists comprises the steps of:

determining a state associated with the determination of the at least two sequential random values;

comparing values of counters utilized in determining the at least two sequential random values; and

detecting a collision based on the determined state and the compared values.

4. (Original) The method of Claim 3, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the step of detecting a collision comprises the steps of:

detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

detecting a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

detecting a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

5. (Original) The method of Claim 4, wherein the step of modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box comprises the steps of:

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

6. (Original) The method of Claim 2, further comprising the steps of:

determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the

common S-box utilized to determine a second portion of the first of the two sequential random values; and

determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the second of the two sequential random values.

7. (Previously presented) The method of Claim 6, wherein the step of determining if a collision exists comprises the steps of:

determining a state associated with the determination of the at least two sequential random values;

comparing values of counters utilized in determining the at least two sequential random values; and

detecting a collision based on the determined state and the compared values.

8. (Original) The method of Claim 7, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the steps of determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values and determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the second of the two sequential random values comprises the steps of:

detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

detecting a second collision if the determined state is the second state and the second t counter values equals the second i counter value.

9. (Original) The method of Claim 8, wherein the step of modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box comprises the steps of:

utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and

utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.

10. - 15. (Canceled)

16. (Currently amended) A system for determining random values for ~~an~~ a stream cipher, comprising:

a memory containing an S-box; and

means for determining at least two sequential random values ~~for the stream cipher~~ in parallel utilizing the S-box~~, the stream cipher comprising a logical combination of the random values and plaintext~~.

17. (Original) The system of Claim 16, wherein the means for determining at least two sequential random values in parallel utilizing the S-box further comprises:

means for determining if a collision exists between accesses of the S-box utilized to determine a first of the two sequential random values and accesses of the S-box utilized to determine a second of the two sequential random values; and

means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box.

18. (Previously presented) The system of Claim 17, wherein the means for determining if a collision exists comprises:

means for determining a state associated with the determination of the at least two sequential random values;

means for comparing values of counters utilized in determining the at least two sequential random values; and

means for detecting a collision based on the determined state and the compared values.

19. (Original) The system of Claim 18, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein means for detecting a collision comprises:

means for detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

means for detecting a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

means for detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

means for detecting a fourth collision if the determined state is the second state, the second j counter values equals the first t counter value; and

means for detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

20. (Original) The system of Claim 19, wherein the means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

means for utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

means for utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

means for utilizing an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value

corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

21. (Original) The system of Claim 17, further comprising:

means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values; and

means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values.

22. (Previously presented) The system of Claim 21, wherein the means for determining if a collision exists comprises:

means for determining a state associated with the determination of the at least two sequential random values;

means for comparing values of counters utilized in determining the at least two sequential random values; and

means for detecting a collision based on the determined state and the compared values.

23. (Original) The system of Claim 22, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the means for determining if a collision exists between accesses of the S-box utilized to determine a first

portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values and the means for determining if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values comprises:

means for detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

means for detecting a second collision if the determined state is the second state and the second t counter values equals the second i counter value.

24. (Original) The system of Claim 23, wherein the means for modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

means for utilizing an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and

means for utilizing an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.

25. (Currently amended) A computer program product for determining random values for an stream cipher, comprising:

a computer readable media having computer readable program code embodied therein, the computer readable program code comprising:

~~computer readable program code configured to provide~~ a memory containing an S-box; and

computer readable program code configured to determine at least two sequential random values ~~for the stream cipher~~ in parallel utilizing the S-box~~, the stream cipher comprising a logical combination of the random values and plaintext~~.

26. (Original) The computer program product of Claim 25, wherein the computer readable program code configured to determine at least two sequential random values in parallel utilizing the S-box further comprises:

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first of the two sequential random values and accesses of the S-box utilized to determine a second of the two sequential random values; and

computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box.

27. (Previously presented) The computer program product of Claim 26, wherein the computer readable program code configured to determine if a collision exists comprises:

computer readable program code configured to determine a state associated with the determination of the at least two sequential random values;

computer readable program code configured to compare values of counters utilized in determining the at least two sequential random values; and

computer readable program code configured to detect a collision based on the determined state and the compared values.

28. (Original) The computer program product of Claim 27, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the computer readable program code configured to detect a collision comprises:

computer readable program code configured to detect a first collision if the determined state is the first state and the second i counter values equals the first j counter value;

computer readable program code configured to detect a second collision if the determined state is the first state and the second j counter values equals the first i counter value;

computer readable program code configured to detect a third collision if the determined state is the first state and the second j counter values equals the first j counter value;

computer readable program code configured to detect a fourth collision if the

determined state is the second state, the second j counter values equals the first t counter value; and

computer readable program code configured to detect a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.

29. (Original) The computer program product of Claim 28, wherein the computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

computer readable program code configured to utilize an S-box value corresponding to the first i counter as the S-box value corresponding to the second i counter if the first collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the first j counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first j counter to a location in the S-box corresponding to the first i counter if the second collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the first i counter as the S-box value corresponding to the second j counter and preventing writing an S-box value corresponding to the first i counter to a location in the S-box corresponding to the first j counter if the third collision is detected;

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fourth collision is detected; and

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the first t counter if the fifth collision is detected.

30. (Original) The computer program product of Claim 26, further comprising:

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of

the two sequential random values; and

computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values.

31. (Previously presented) The computer program product of Claim 30, wherein the computer readable program code configured to determine if a collision exists comprises:

computer readable program code configured to determine a state associated with the determination of the at least two sequential random values;

computer readable program code configured to compare values of counters utilized in determining the at least two sequential random values; and

computer readable program code configured to detect a collision based on the determined state and the compared values.

32. (Original) The computer program product of Claim 31, wherein at least two states are associated with the determination of the at least two sequential random values, wherein the counters associated with at least two sequential values comprise first and second i counter values, first and second j counter values and first and second t counter values and wherein the computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the S-box utilized to determine a second portion of the first of the two sequential random values and the computer readable program code configured to determine if a collision exists between accesses of the S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the S-box utilized to determine a second portion of the second of the two sequential random values comprises:

computer readable program code configured to detect a first collision if the determined state is the second state and the first i counter value equals the first t counter value; and

computer readable program code configured to detect a second collision if the

determined state is the second state and the second t counter values equals the second i counter value.

33. (Original) The computer program product of Claim 32, wherein the computer readable program code configured to modify the determination of the at least two sequential random values based on whether a collision exists between accesses of the S-box comprises:

computer readable program code configured to utilize an S-box value corresponding to the first j counter as the S-box value corresponding to the first t counter if the first collision is detected; and

computer readable program code configured to utilize an S-box value corresponding to the second j counter as the S-box value corresponding to the second t counter if the second collision is detected.